Technical Cybersecurity

Cybersecurity Today: Ransomware

What is Ransomware?

WHY STEAL INFORMATION?

- Just encrypt it and hold it for ransom

WHY DOES IT WORK?

- People value digital assets
- …and they don’t back them up very well
- …and they don’t protect those backups if they do

Who’s Affected?

Consumers

- Most strains of ransomware were built with mass consumer targets in mind
- Some have crossed into enterprises though

Enterprise

- Ransomware is even more damaging to companies
- This may be an area for growth; consumers rarely pay, but enterprises frequently do

Not Very Successful

Encryption is hard

- Sure, AES256 is virtually unbreakable, but how to you manage the keys?

Many strains don't decrypt

- One strategy to handle key management is to not manage them
- …but then folks learn that you're not only a criminal, you're dishonest :-)

Example: Wannacry

DELIVERY

- Weaponized PDF or email
- Dropper on system, contacts domain killswitch, installation

PERSISTENCE

- Registry keys, windows service

ENCRYPTION, NOTIFICATION

- Searches for a wide variety of files, encrypts them, notifies user

Example: Wannacry

USES TOR FOR COMMUNICATION

- Anonymity, privacy

AES128, RSA PUBLIC/PRIVATE

- Two public keys distributed
- One key pair generated
- AES128 used on files, key protected with generated public key
- Attacker encrypts private keys associated with distributed public keys

How about exploit kits?